

CLAIMS

Now, therefore, the following is claimed:

1 1. A computer system comprising:
2 memory; and
3 a security application configured to lock down resources of said computer system
4 by modifying a machine state of said computer system in response to a request for
5 activating a first security profile, said security application configured to store data
6 indicative of said machine state in said memory in response to said request for activating
7 said first security profile, said security application configured to modify said machine state
8 in response to a request for activating a second security profile, said security application
9 configured to retrieve said data in response to a request for recovering said first security
10 profile and to modify said machine state based on said retrieved data.

1 2. The system of claim 1, wherein said security application includes default
2 data defining default levels of security, wherein said security application enables a user to
3 select one of said default levels of security, and wherein said security application is
4 configured to modify said machine state in response to said request for activating said first
5 security profile based on said selected default level of security.

1 3. The system of claim 2, wherein said security application defines a plurality
2 of rules for locking down said computer system, wherein said security application
3 configured to enable ones of said rules based on which of said default levels is selected by
4 said user, and wherein said security application is further configured to cause said
5 computer system to enforce each enabled rule within said plurality of rules by modifying
6 said machine state in response to said request for activating said first security profile.

1 4. The system of claim 3, wherein said security application enables said user
2 to change which of said rules are enabled.

1 5. A computer system, comprising:
2 memory; and
3 a security application defining a plurality of rules, said security application
4 configured to enable a user to select a set of said rules for enforcement by said computer
5 system, said security application configured to lock down said computer system by
6 causing said computer system to enforce said selected set of rules in response to an
7 activation request, said security application further configured to store data identifying
8 said selected set in response to said activation request, said security application configured
9 to change which of said plurality of rules are enforced by said computer system based on
10 inputs to said computer system, said security application configured to retrieve said data in
11 response to a user request and to automatically identify said set of rules based on said
12 retrieved data, said security application further configured to cause said computer system
13 to enforce said identified rules in response to said user request.

1 6. The system of claim 5, wherein said security application is further
2 configured to define multiple sets of default data, each of said sets of default data
3 identifying different ones of said rules as being enabled for enforcement, said security
4 application configured to enable said user to select one of said sets of default data and to
5 determine which of said rules are selected for inclusion into said selected set of rules based
6 on which of said rules are indicated as enabled.

1 7. The system of claim 6, wherein said security application enables said user
2 to change which of said rules are indicated as being enabled.

1 8. A computer system comprising:
2 means for storing data; and
3 means for locking down resources of said computer system by modifying a
4 machine state of said computer system in response to a request for activating a first
5 security profile, said locking down means including a means for storing security profile
6 data indicative of said machine state in said memory in response to said request for
7 activating said first security profile, said locking down means including a means for
8 modifying said machine state in response to a request for activating a second security
9 profile, said locking down means including a means for retrieving said security profile data
10 in response to a request for recovering said first security profile and for modifying said
11 machine state based on said retrieved data.

1 9. A method for locking down resources of a computer system, comprising
2 the steps of:
3 receiving a request for activating a first security profile;
4 modifying a machine state of said computer system in response to said request for
5 activating said first security profile;
6 storing data indicative of said machine state in response to said request for
7 activating said first security profile;
8 modifying said machine state in response to a request for activating a second
9 security profile;
10 retrieving said data in response to a request for recovering said first security
11 profile; and
12 modifying said machine state based on said retrieved data in response to said
13 request for recovering said first security profile.

1 10. The method of claim 9, further comprising the steps of:
2 defining default levels of security; and
3 selecting one of said default levels of security,
4 wherein said modifying step that is performed in response to said request for
5 activating said first security profile is based on said selecting step.

1 11. The method of claim 10, further comprising the steps of:
2 defining a plurality of rules for locking down said computer system;
3 associating each of said default levels of security with different ones of said rules;
4 enabling ones of said rules based on which of said rules are associated, via said
5 associating step, with said default level selected in said selecting step; and
6 enforcing each of said rules enabled via said enabling step based on said machine
7 state as modified via said modifying step that is performed in response to said request for
8 activating said first security profile.

1 12. The method of claim 11, further comprising the step of:
2 enabling a user to change which of said rules are enabled.

1 13. A method for locking down resources of a computer system, comprising
2 the steps of:
3 defining a plurality of rules for locking down said computer system;
4 receiving an input from a user of said computer system;
5 selecting a set of said rules based on said input;
6 causing said computer system to enforce said selected set of rules in response to an
7 activation request;
8 storing data identifying said selected set of rules in response to said activation
9 request;
10 changing which of said plurality of rules are enforced by said computer system;
11 retrieving said data in response to a user request;
12 automatically identifying said selected set of rules based on said retrieved data; and
13 causing said computer system to enforce said selected set of rules in response to
14 said user request.

1 14. The method of claim 13, further comprising the steps of:
2 defining multiple sets of default data, each of said sets of default data identifying
3 different ones of said rules as being enabled; and
4 selecting one of said sets of default data,
5 wherein said selecting a set of said rules step is further based on which of said sets
6 of default data is selected via said selecting one of said sets of default data step.